A1 cont. cycles are used to concurrently perform an additional limited modular multiplication operation where two of three operands, B and M, must be the same.--

Please replace paragraph 30 beginning on page 11 with the following rewritten paragraph:

--In the embodiment illustrated in **Figure 2**, rather than utilize the first and second independent computation channels to perform two distinct modular multiplication operations, the computation channels are combined to form a single "virtual" computation chain according to the present invention by feeding the end of the linear systolic array of processing elements back into the beginning of the array. The second computation channel is consequently utilized as a continuation of the first, effectively doubling the length of the linear systolic array while sacrificing one of the available multiplication channels. It should be appreciated however that in alternative embodiments of the invention the resulting effective linear systolic array length may be greater than or less than twice the original length. For example, embodiments of the invention may be implemented, in which a linear systolic array having more than two independent computation channels is utilized resulting in a longer effective array length. Similarly, an embodiment in which not all processing elements of a linear systolic array are utilized or included within the provided feedback loop may be implemented resulting in a shorter effective array length.--

A2

Please replace paragraph 33 beginning on page 12 with the following rewritten paragraph:

--Consequently, the static fed-back modular multiplier embodiment illustrated in **Figure 2** may be utilized to perform an n-bit modular multiplication operation using a linear systolic array having a number of processing elements ordinarily sufficient to perform an n/2-bit modular multiplication operation. For purposes of this description therefore, the processing elements of the illustrated array or chain will be referred to by number from 0 to N/2 + 2 from left to right starting with the first processing element, where N is equal to the number of digits within the operands processed in the modular multiplication. So for example, a 1024-bit modular multiplication operation, ordinarily requiring 259 4-bit processing elements plus end logic (i.e. 1024 / 4 = N = 256 + 3 additional PEs = 259) would instead require 131 4-bit processing elements (N = 256 / 2 = 128 + 3 = 131). In one embodiment of the present invention, a

A3